LÄHIVERKON SUUNNITTELU

YRITYKSELLE

Kari Ainonen

Opinnäytetyö
Toukokuu 2013
Tietotekniikka
Tietoliikennetekniikka ja tietoverkot

TAMPEREEN AMMATTIKORKEAKOULU
Tampere University of Applied Sciences

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietotekniikka
Tietoliikennetekniikka ja tietoverkot

KARI AINONEN:
Lähiverkon suunnittelu yritykselle

Opinnäytetyö 34 sivua, joista liitteitä 2 sivua
Toukokuu 2013

Lähiverkon suunnittelussa tärkeintä on toteuttaa verkko, joka vastaa yrityksen tarpeisiin. Näistä tarpeista tärkein ja suunnittelun kulmakivi oli tarjottavat palvelut. Verkon tarvitsee vastata näiden palveluiden vaatimuksiin niin laitteiden kuin kaapeloinnin osalta. Tavoitteena oli tarjota palvelut mahdollisimman pienellä aktiivilaitemäärällä.

Suunnittelun lopputuloksena oli siis toimiva lähiverkko, jota yritys pystyy hyödyntämään mahdollisimman tehokkaasti. Nykyisin yleisin suunnittelussa käytettävä malli on Ciscon kolmitasoinen hierarkiamalli. Tällä mallilla saadaan jaettua palvelut verkon eri tasoille, joka vähentää kuormitusta sekä mahdollisia pullonkauloja. Nämä tasot ovat liityntä-, jakelu-, ja ydintaso. Jokaisella tasolla on omat palvelunsa, joita yrityksessä käytetään. Yleisohjeena pidetään, että liityntätasolla on työasemat, tulostimet sekä mahdolliset tiimikohtaiset palvelimet. Tyypillisesti jakelutasolla on hakemistopalvelimet, autentikointipalvelimet sekä toimipaikkakohtaiset tiedosto- ja sovelluspalvelimet. Ydintasolta löytyvät niin sanotut julkiset palvelut, kuten web-palvelin, nimipalvelin ja sähköpostipalvelin, joita suojaavat palomuurit. Ydintasolle kuuluvat myös toimipaikkojen väliset yhteydet sekä toimipaikkojen internet-yhteyksien järjestäminen.

Suunnittelussa on käytetty lähtökohtana Ciscon hierarkiamallia ja luotettavaa alan kirjallisuutta sekä verkkojulkaisuja. Työn painopiste oli lähiverkkojen määrittely- ja suunnitteluvaiheessa, joissa käsiteltiin yrityksen tarpeita ja palveluita. Tuloksia tarkasteltaessa huomataan, että suunnittelulla saatiin aikaan perusmalli, jota laajentamalla ja tarkentamalla voidaan yrityksen verkko päivittää vastaamaan nykyisiä tarpeita.

Asiasanat: lähiverkko, suunnittelu, tietoverkko, cisco, ppdioo

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
ICT Engineering
Telecommunications Engineering and Networks

KARI AINONEN:
Designing a Local Area Network for a Corporation

Bachelor's thesis 34 pages, appendices 2 pages
May 2013

Design of local area network the most important thing is to implement a network that meets the company's needs. Of these, the most important needs and the design of the cornerstone of the services offered. The network needed to answer these services sees the requirements to devices other than the cabling. The aim was to provide the services with a minimum number of active devices.

The design, therefore, the end result was a functional local area network, which the company is able to utilize as efficiently as possible. Currently, the most common type used in the design model is the Cisco three-layered hierarchical model. This model will be delivered to the network services at different layer, which reduces the load and potential bottlenecks. These layers are the access, distribution, and core layer. Each layer has its own services, which the company used. A general guideline is considered that in the access layer have workstations, printers and possible team-based servers. Typically, the distribution layer has directory servers, authentication servers, as well as site-file and application servers. The core layer can be found in the so-called public services, such as web server, DNS server, and mail server, which are protected by firewalls. The core layer has also links between branch, as well as internet connectivity of these offices.

The design has been based on the Cisco hierarchical model and reliable field-recorded literary, as well as online publications. The focus of local area networks for implement and design stage, dealing with the company's needs and services. Examining the results, it was found that the design achievement is the basic model. An expanding and by specifying a company's network can be updated to meet current needs.

Key words: local area network, designing network, data network, cisco, ppdioo

SISÄLLYS

LYHENTEET JA TERMIT

BOOTP	Bootstrap protokolla, joka hakee asiakaskoneelle internet protokollan osoitteen, käytetään yleensä silloin, kun työasemassa ei ole kiintolevyä.
DHCP	Dynamic Host Configuration Protocol, jonka pääasiallinen tehtävä on jakaa IP-osoitteita verkon laitteille annetusta osoitealueesta
DNS	nimipalvelin, johon asetetaan mm. yrityksen web-sivun osoite nimellä
DSL	Digital Subscriber Line, jota käytetään mm. internet-yhteyksissä koteihin
Elinkaariajattelumalli	Ciscon Lifecycle PPDIOO malli verkon uudistamisesta
FTP	File Transfer Protocol on tiedonsiirto protokolla, joka hyödyntää TCP-protokollaa ja toimii asiakas-palvelin periaatteella
HTTP	Hypertext Transfer Protocol eli hypertekstin siirtoprotokolla, jota käyttävät selaimet ja web-palvelimet tiedonsiirtoon
IDS	Intrusion Detection System eli tunkeutumisen havaitsemisjärjestelmä, kaksi päätyyppiä verkko- (NIDS) ja isäntäpohjainen (HIDS)
IP	Internet protokolla, jolla koneet yhdistetään internetiin
Konfiguraatio	On verkkolaitteiden asetusten asettamista halutunlaiseksi
Kytkin	Moniporttinen laite, johon tietokoneet liitetään
MAC-osoite	Media Access Control on laitteiden ns. fyysinen osoite, joka koostuu 6-tavuisesta numerokirjain yhdistelmästä
NAT	Network Address Translation eli muuntaa julkisen IP-osoitteen yrityksen sisäiseksi IP-osoitteeksi
Palomuuri	Suojaa verkkoa hyökkäyksiltä
PPDIOO	Prepare, Plan, Design, Implement, Operate, Optimize suomennettuna esitutkimus, määrittely, suunnittelu, toteutus, käyttöönotto ja optimointi/ylläpitö, Ciscon elinkaariajattelumallin eri vaiheet

POP3	Post Office Protocol versio 3 on sähköpostin vastaanottava protokolla
PPP	Point-to-Point Protocol käytetään luomaan yhteyksiä kahden verkkolaitteen välille
Reititin	Vastaa tiedon kulusta toiseen verkkoon
SMTP	Simple Mail Transfer Protocol eli lähettävä sähköpostin protokolla
SSH	Secure Shell on tarkoitettu salattuun yhteyden ottoon esim. kytkimille ja reitittimille
TCP	Transmission Control Protocol on protokolla, jolla luodaan yhteyksiä tietokoneiden välille
TELNET	yhteys protokolla, jolla voidaan hallita verkon yli esim. reitittimiä tai kytkimiä, ei salattu
VLAN	Virtuaalinen lähiverkko, jolla pystytään jakamaan esim. työryhmät tai osastot omiksi yksiköikseen
VPN	Virtuaalinen yksityinen verkko eli muodostetaan kahden pisteen välille suojattuyhteys

1 JOHDANTO

Tämän työn tarkoituksena on perehtyä tietoverkon suunnittelun erivaiheisiin. Perustana käytetään Ciscon kolmitasoista verkkojärjestelmä tasomallia, jota omien näkemyksien mukaan muokataan. Verkon suunnittelu jaetaan kolmeen päävaiheeseen määrittäminen, suunnittelu sekä ylläpito ja kehittäminen. Nämä vaiheet voidaan jakaa vielä pienemmiksi osa-alueiksi esimerkiksi Ciscon verkon elinkaariajattelumallin avulla. Tätä mallia sovelletaan verkon ylläpitoon ja kehittämiseen, jotta verkko vastaa myös tulevaisuudessa yrityksen tarpeisiin. Liitteessä 1 on looginen topologia malli yrityksen tulevasta verkosta.

OSI-mallin avulla yritetään selventää eri laitteiden tarkoitusta verkossa sekä miten verkko toimii. Suunnittelussa otetaan huomioon verkon käyttötarkoitus ja tulevaisuuden mahdolliset laajentumisen tarpeet sekä kustannukset. Liitteessä 2 on malli kustannuslaskelmasta.

Työssä käsitellään myös tietoturvaa sekä ylläpitoa hyvin pintapuolisesti. Nämä ovat oleellinen osa verkkoa ja perusta näiden toteuttamiseen luodaan suunnitteluvaiheessa. Seuraavat vaiheet suunnittelun jälkeen olisivat toteutus, testaus ja käyttöönotto, mutta nämä jäävät pois resurssien puutteen vuoksi.

Yritys on kuvitteellinen ja kaikki tiedot yrityksestä sekä lähiverkosta ovat keksittyjä.

2 VERKON MÄÄRITTÄMINEN

2.1 Yritys Oy

Yrityksessä työskentelee 90 ihmistä eri osastoissa. Osastot on jaettu seuraavasti hallinto, myynti, markkinointi ja varasto. Tämä yritys on perustettu 90-luvun alkupuolella ja heidän tietoverkkonsa infrastruktuuri on vanhentunut. Sitä on paranneltu vuosien varrella mutta siitä on tullut tilkkutäkki, jota on vaikea enää hallinnoida. Myös verkon hitaus ja ylläpito kustannukset ovat kohtuuttoman suuret.

Nämä ovat olleet lähtökohdat yrityksen johdolle, joka on päättänyt uudistaa koko käytössä olevan verkon. Se rakennetaan olemassa olevan rinnalle ja kytketään testauksen jälkeen päätoimiseksi verkoksi. Tämän jälkeen vanha verkko puretaan. Yrityksen johto on kilpailuttanut hankkeen. He ovat tilanneet suunnitelman sekä kustannusarvion uudesta verkosta.

Vaatimuksena on ollut, että käytetään Ciscon laitteita, jotta säästytään henkilökunnan kouluttamiselta. Sekä luonnollisesti verkon käytettävyys, nopeus sekä vikasietoisuus paranevat. Tietoturvaan parannetaan uudessa verkossa huomattavasti.

2.2 Mitä tietoverkko sisältää?

Verkko koostuu pääsääntöisesti kahdesta eri laitteesta, jotka tunnetaan nimillä kytkin ja reititin. Käyttäjien tietokoneista käytetään nimitystä loppukäyttäjä, asiakaskone tai työasema sekä palveluja tarjoavista tietokoneista palvelin. Verkosta voi löytyä myös palomuuri tai reititin voi toimia sellaisena. Palomuurin tarkoitus on pitää tunkeilijat poissa verkosta. Näiden laitteiden sekä verkossa toimivien protokollien toimintaa selvennetään OSI-mallin avulla.

2.2.1 OSI-malli

Open Systems Interconnection Reference Model kuvaa tiedonsiirtoprotokollien yhdistelmän seitsemässä eri kerroksessa. Kerrokset tarjoavat palveluja toiselle kerrokselle. OSI-malli on kehitetty 1980-luvun alussa ja se on ISO:n (International Organization for Standardization) hyväksymä kansainvälinen standardi. Kuviosta 1 havainnoidaan mitä kerrosta verkon laitteet hyödyntävät.

KUVIO 1. OSI-malli (http://fi.wikipedia.org/wiki/OSI-viitemalli, muokattu)

Fyysinenkerros (Physical Layer) määrittää fyysisen ja sähköisen tunnusmerkit, kuten sähkökaapelin, valokuidun tai radioaallon yli tapahtuvan siirron. Loppujen lopuksi kaikki tieto kulkee kaapelissa vain ykkösinä ja nollina. (Briscoe, N. 2000, 13–14.)

Siirtokerros (Data Link Layer) määrittää tiedon jakamiseen tarvittavat parametrit. Verkon aktiivilaitteet, kuten verkkokortit, kytkimet ja sillat kuuluvat tähän kerrokseen. Tätä kerrosta käyttävät mm. protokollat PPP, MAC ja DSL, joista jälkimmäistä käytetään nykyään internet-yhteyden muodostamiseen. Ethernet ohjaa MAC-osoitteita, jotka ovat yksilöllisiä jokaisella laitteella. Tämän avulla kytkimet oppivat nopeasti verkon topologian, missä portissa mikäkin laite sijaitsee. (Briscoe, N. 2000, 13–14.)

Verkkokerros (Network Layer) tarjoaa välineet ottaa yhteyden, ylläpitää yhteyttä ja katkaista yhteyden muiden järjestelmien kanssa. Protokollista IP on käytetyin sekä jotkut

reititysprotokollat käyttävät verkkokerrosta. Kaikki reitittimet operoivat tällä kerroksella. (Briscoe, N. 2000, 13–14.)

Kuljetuskerros (Transport Layer) standardin mukaan kuljetuskerros vähentää istuntokerroksen taakkaa tiedon varmistamisesta sekä eheydestä. Protokollista TCP on käytetyin tällä kerroksella. TCP vastaa lähetyksen menosta perille sekä mahdollisesta uudelleen lähetyksestä. (Briscoe, N. 2000, 13–14.)

Istuntokerros (Session Layer) mahdollistaa kahden eri tahon kommunikoinnin keskenään. Esimerkiksi verkkokaupassa, kun ostoskoriin lisätään tuotteita, on tärkeää, ettei kaistantasaaja (load-balanced) siirrä toiselle palvelimelle kesken ostotapahtuman. (Briscoe, N. 2000, 13–14.)

Esityskerros (Presentation Layer) nimensä mukaisesti tekee muunnoksia esitystapaan. Sovellus data pakataan tai puretaan, protokolla konversiot, salaukset tai salauksen purkamiset sekä grafiikka muunnokset. (Briscoe, N. 2000, 13–14.)

Sovelluskerros (Application Layer) tarjoaa käyttöliittymän. Täällä operoivat käyttäjät ja sovellus protokollat kuten telnet, http, ftp ja sähköposti POP3 ja SMTP (Briscoe, N. 2000, 13–14.)

2.2.2 Tietoverkon komponentit

Kuten OSI-mallista käy ilmi, kytkinten ensisijainen tarkoitus on siirtää dataa portista toiseen. Tietokoneen lähettäessä dataa sen ympärille luodaan kehys. Kytkin saa kehyksestä selville lähettäjän MAC-osoitteen sekä portin ja lisää ne omaan tauluunsa. Kun taulussa on kaikkien laitteiden portit ja osoitteet, vähentää tämä huomattavasti ylimääräistä liikennettä verkossa. On olemassa kytkimiä, joihin on lisätty kerroksen 3 reititys. Näitä voidaan hyödyntää korvaamaan reitittimiä yrityksen runkoverkossa. (Lammle 2011, 4.)

Reitittimen tarkoitus on yhdistää eri osoitteiden omaavia verkkoja toisiinsa. Kun tietokone lähettää dataa toiseen verkkoon yllä mainitun kehyksen ympärille luodaan ip-osoitteet ja tätä kokonaisuutta kutsutaan paketiksi. Reitittimet ovat verkon monitoimi-

laitteita. Ne voidaan konfiguroida toimimaan palomuurina, jakamaan ip-osoitteita tai muuntamaan ip-osoitteita. Reitittimet toimivat OSI-mallin kerroksella 3. (Lammle 2011, 2–4.)

2.2.3 Tietoverkon kaapelointi

Tänä päivänä kaapeloinnilla on iso merkitys tiedonsiirrossa. Tekniikat kehittyvät huimaa vauhtia ja nopeudet kasvavat niin kuin myös tarvittava kaistanleveys. Yleisin käytettävä lähiverkon kaapelointi tekniikka on Ethernet, jolla päästään jo 100 gigabitin tiedonsiirto nopeuteen sekunnissa. Tämähän on teoreettinen maksimi mutta käytännössä noin kymmenesosa on todellinen nopeus nykypäivän laitteilla. (Pitkänen, J. 2010)

Alati kasvavat tiedonsiirto määrät tekevät kaapeloinnista haastavaa varsinkin tulevaisuutta ajatellen. Video konferenssit säästävät matkakuluja sekä aikaa mutta tuovat kustannuksia IT-infrastruktuuriin. Ongelmana varsinkin vanhemmissa taloissa on kaapelointi, josta muodostuu pullonkaula tiedonsiirron osalta. (Pitkänen, J. 2010)

Hyvän tietoverkon suunnittelijan on lähestulkoon oltava sukua oraakkelille, jotta pystyy suunnittelemaan riittävän nopean kaapeloinnin. Nyrkkisääntönä voidaan pitää, että työasemille vedetään Ethernet ja runkoverkkoon valokuitua. Nykyään valokuitukaapelilla laboratorio olosuhteissa on saavutettu lähes valonnopeus, kun nopeutta verrataan valonnopeuteen tyhjiössä. Tekniikka ei vielä ole valmis pitkille matkoille suuren tietohävikin vuoksi mutta sitä voidaan käyttää suurissa datakeskuksissa laitteiden väliseen tiedonsiirtoon. Tässä uudessa ”ilmakuidussa” on 37 laajakaistaista kanavaa, joista kukin pystyy välittämään 40 gigabittiä sekunnissa. Täten kaapelin kokonaiskapasiteetti on 1,48 terabittiä sekunnissa. (Digitoday: Pure pölyä valokuitu: tieto kiitää melkein valon nopeudella ilmakuidussa 2013.)

2.3 Tietoverkon tarpeet yrityksessä

Määrittelyvaiheessa tarkoituksena on selvittää tietoverkon ominaisuudet. Tähän vaiheeseen liittyvät vahvasti erilaiset kartoitukset ja analyysit. Olennaisesti määrittelyvaiheen sisältöön vaikuttaa, ollaanko rakentamassa täysin uutta tietojärjestelmäverkkoa vai kor-

vataanko aiempi järjestelmä uudella, tehokkaammalla järjestelmällä, kuten tässä tapauksessa. (Hakala & Vainio 2005, 407.)

Määrittelyn apuna käytetään usein tarvekartoituksia, joissa kysytään tietojärjestelmän käyttäjien tarpeita ja mahdollisia toiveita. Näitä verrataan yrityksen liiketoiminta- ja aiempiin IT-suunnitelmiin. Kartoituksien analysointiin tarvitaan monien tahojen näkemyksiä, mm. käyttäjien, tietotekniikan ja tietojenkäsittelyn asiantuntijoiden sekä erityisesti yrityksen johdon panosta. Johdolta edellytetään sitoutumista projektiin, ja tämä varmistetaan käyttämällä ohjausryhmässä ylimmän johdon edustajia. Peruskäyttäjien mukaan ottaminen auttaa heitä ymmärtämään uudistuksia ja tätä kautta vähentää muutosvastarintaa. (Hakala & Vainio 2005, 407.)

Määrittelyn työkalut ovat erilaiset analyysit. Seuraavaksi käydään läpi oleellisimmat niistä. Täysin uutta tietojärjestelmää rakennettaessa keskeisimmät analyysit ovat tietotarve-, tietovarasto- ja tietovuoanalyysi. Mikäli kyseessä on vanhemman tietojärjestelmän päivitys tai korvaaminen tehokkaammalla järjestelmällä, tehdään yleensä edellisten lisäksi ongelma- ja syy-seuraus-analyysit. (Hakala & Vainio 2005, 407.)

2.4 Tietoverkon analyysit

Tietotarveanalyysissä määritellään, mitä tietoja yrityksen eri toimintaprosessit tarvitsevat. Tiedot luokitellaan syöttö- ja tulostustietoihin. Syöttötiedot ovat tietojärjestelmään syötettäviä yksittäisiätietoja, esim. asiakkaiden yhteystiedot, ostohistoria tai luottotiedot. Tulostustietoja ovat näistä tietojenkäsittelyn avulla johdettuja erilaiset raportit ja yhteenvedot. Myös erilaiset sopimuksiin ja lainsäädäntöön perustuvat tulosteet, kuten laskut ja kirjanpitomateriaali luetaan tulostietoihin. (Hakala & Vainio 2005, 408.)

Tietotarveanalyysiä täsmennetään edelleen jakamalla tiedot tietoturvapolitiikan mukaisiin luokkiin. Yrityksen tietoturvaluokitus määrittelee tietojen luottamuksellisuuden ja saatavuuden organisaation toiminnan jatkuvuuden kannalta. Tietovarastoanalyysissä pohditaan tietotarveanalyysissä löydettyjen tietojen säilyttämistä. Tietojen luonteen perusteella pyritään määrittämään niille sopiva tallennusmuoto, joka voi olla relaatio- tai dokumenttitietokanta, tiedostomuotoinen tallennus tai tulostus. Tulostus voi tapahtua esim. paperille, levyille jne. Varastointitavan määrittelyn yhteydessä tarkistetaan sen

soveltuvuus sekä tietojen saatavuuden että luottamuksellisuuden suhteen. (Hakala & Vainio 2005, 408.)

Tietovuoanalyysissä selvitetään, miten tiedot kulkevat yrityksessä. Tarkastelu suoritetaan yrityksen eri toimintaprosessien sisällä ja niiden välillä. Tietovuoanalyysissä tiedot luokitellaan raportoivaan, ohjaavaan ja rutiinitietoon. Raportoiva tieto kulkee tyypillisesti alemmilta tasoilta ylemmille tasoille. Ohjaava tieto puolestaan kulkee ylhäältä alas. Nykyaikaisessa yrityksessä työntekijöiden toimintaa ohjaava tieto ja toiminnan tuloksellisuudesta kertova raportoiva tieto eivät välttämättä kulje virallisen organisaatiokaavion mukaisesti. Todellisen tiedonkulun luokittelu edellyttää niin sanotun epävirallisen organisaationkaavion selvittämistä. (Hakala & Vainio 2005, 408.)

Tietovuoanalyysissä pitäisi pohtia, miten tietoa tarvitsevat henkilöt saavat tiedon eri tietovarastoista. Tehdäänkö tietovarastoon, esimerkiksi tietokantaan, säännöllisesti kyselyitä vai tarvitaanko automaattista ilmoitusta tiedon syntymisestä. Ongelma-analyysillä pyritään selvittämään vanhan tietojärjestelmän puutteita. Miksi järjestelmä ei toimi riittävän tehokkaasti, mitä puutteita sen ylläpitämissä tiedoissa on, onko järjestelmässä tietoturvaongelmia jne. Syy-seuraus-analyysillä pyritään löytämään aiemman tietojärjestelmän puutteet ja heikkoudet. (Hakala & Vainio 2005, 408.)

Tietoverkkosuunnittelussa määrittelyvaiheen analyyseihin kuuluvat myös verkon liikenneanalyysit. Nykyisen verkon liikennemäärät mitataan ja luokitellaan sovelluksittain ja toimintaprosesseittain. Tietotarve-, tietovarasto- ja tietovuoanalyysien avulla pyritään määrittämään uuden verkon aiheuttaman liikenteen määrä. Verkon suunnittelussa liikenneanalyysin päätarkoituksena on määritellä eri verkon osien kapasiteettivaatimukset. (Hakala & Vainio 2005, 408–409.)

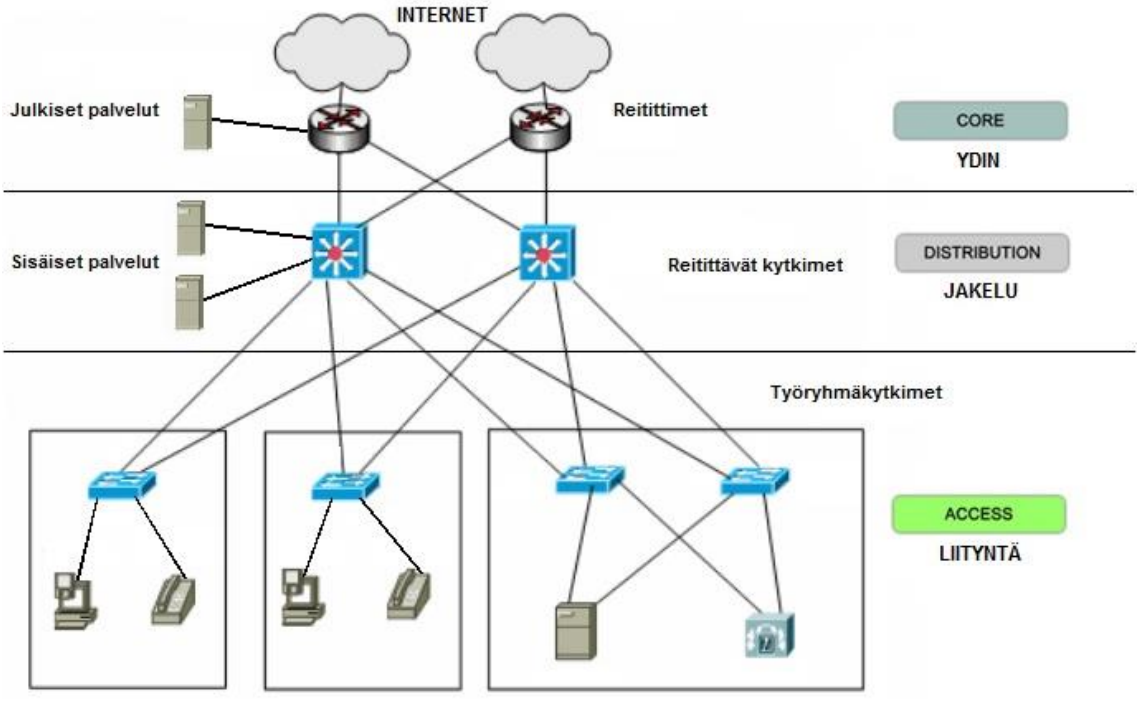
Määrittelyvaiheen tarkoituksena on löytää vastaus ”mitä ominaisuuksia tietojärjestelmällä pitää olla?” Tietoverkon osalta se kertoo tiedonsiirronkapasiteetin, vikasietoisuuden sekä luottamuksellisuuden mitä eri verkon osissa edellytetään. Järjestelmältä edellytettävät ominaisuudet kirjataan määrittelydokumenttiin, joka hyväksytetään projektin ohjausryhmällä. (Hakala & Vainio 2005, 409.)

3 VERKON SUUNNITTELU

3.1 Verkon rakenne

On hyvin harvinaista, että yritykset uusivat koko verkkonsa kerralla. Yleensä sitä uudistetaan pieninä paloina ja se onnistuu hyvin, mikäli verkko on toteutettu loogisesti. Loogisuudella tarkoitetaan verkon jakamista tasoihin ja segmentteihin, joissa on eri ominaisuuksia ja kokonaisuuksia. Tämä myös helpottaa ylläpitämistä ja ongelmien rajausta eri alueille.

Suunnittelun perustana käytetään Ciscon esittelemää kolmitasoista verkkojärjestelmä tasomallia kuviossa 2. Tasot ovat liityntä-, jakelu- ja ydinkerros. Jokaisella tasolla on omat erityistehtävänsä. Verkon rakenteesta olisi hyvä löytyä kaksi erillistä topologiaa, fyysinen ja looginen. Fyysisestä topologiasta ilmenee laitteiden sijainnit sekä johdotuksien kulku rakennuksessa. Yllä mainitut tasot löytyvät loogisesta topologiasta kerroksittain. Looginen topologia on mallinnus verkosta, josta löytyy kaikki tarvittava tieto. Nämä tiedot riippuvat verkosta mutta tässä kyseisessä verkossa siitä löytyvät ip-osoitteet sekä vlan:it ja reititysprotokollat.



KUVIO 2. Verkkojärjestelmän tasomalli keskisuurelle tai suurelle yritykselle

3.1.1 Liityntätaso

Liityntätaso mielletään myös työpöytä kerrokseksi, koska se on lähinnä tavallista tietokoneen käyttäjää. Nimensä mukaisesti tällä kerroksella liitytään yrityksen lähiverkkoon. Tällä kerroksella on käyttäjien työasemat sekä useimmat jaetut oheislaitteet, kuten tulostimet. Työryhmäpalvelimet sekä pienet osastokohtaiset tiedosto- ja sovelluspalvelimet pyritään sijoittamaan tälle kerrokselle. Mahdollisuuksien mukaan myös tulostusjonoja hallinnoivat palvelimet. (Hakala & Vainio 2005, 412.)

3.1.2 Jakelutaso

Jakelutaso mielletään joskus työryhmä kerrokseksi ja se on kommunikointi piste liitynnän ja ytimen välillä. Tälle kerrokselle sijoitetaan suuremmalle käyttäjäjoukolle yhteiset palvelimet. Näitä ovat mm. organisaation toimipaikkakohtaiset palvelimet, suuret osastokohtaiset tiedosto-, sovellus- ja massatulostuspalvelimet sekä erilaiset yhdyskäytäväpalvelimet. Hakemisto-. autentikointi-, intranet- ja sisäiset sähköpostipalvelimet toimivat yleensä jakelutasolla (Hakala & Vainio 2005, 412.)

Näiden lisäksi jakelutaso huolehtii useista muista tehtävistä. Näitä ovat reititys, pääsylistat, pakettisuodatus ja jonotus. Turvallisuus- ja verkkopolitiikat kuuluvat myös, kuten osoitteen muunnokset sekä palomuurit. Reititysprotokollien jakelu toistensa välillä sekä virtuaaliverkkojen- ja muut työryhmäpalvelut. (Lammle 2011, 48.)

3.1.3 Ydintaso

Ydintaso on verkon selkäranka. Tältä tasolta lähtevät yhteydet organisaation muihin toimipaikkoihin sekä internetiin laajaverkkoyhteyksien avulla. Ydintasolle voidaan sijoittaa palvelimia, jotka ovat toimipisteille yhteisiä tai joiden halutaan olevan internetistä käsin käytettävissä. Tyypillisiä palvelimia ovat www- ja ekstranet- sekä ulkoiset sähköpostipalvelimet unohtamatta VPN-palvelimia. (Hakala & Vainio 2005, 412–413.)

Ydintason pääasiallinen tehtävä on reitittää dataa niin nopeasti kuin mahdollista. Jos tällä kerroksella syntyy vika tilanne, se vaikuttaa kaikkiin käyttäjiin alemmilla tasoilla. Siksi on tärkeää huolehtia vikasietoisuudesta sekä pienestä viiveestä. Suositellaan käytettävän reititysprotokollia, joilla on nopea verkonselvittämisen aika. (Lammle 2011, 48.)

3.2 Tasojen käytännön suunnittelu

Kaapelointijärjestelmän, aktiivilaitteiden ja tarvittavien palvelinten suunnittelussa lähdetään yleensä liikkeelle ns. ylhäältä-alas-menetelmällä. Ensin hahmotetaan määrittelyvaiheen tietojen perusteella ydintason palvelut sekä niiden vaatimat laite- ja kaapelointiratkaisut. Tästä edetään jakelutasolle ja viimeisenä liityntätasolle. (Hakala & Vainio 2005, 419.)

3.2.1 Ydintason suunnittelu

Ydintasolle kuuluvat organisaation toimipaikkoja yhdistävät tietoliikenneyhteydet sekä internet-yhteyksien järjestäminen. Lähtökohtina ovat määrittelyvaiheessa selvitetyt kapasiteetti- ja tietoturvallisuustarpeet. Pohjaksi laaditaan looginen topologia, josta ilmenee toimipisteet, julkinen internet ja niiden väliset yhteydet. Topologiaan merkitään yhteyksien kapasiteetit ja protokollatiedot. VPN- ja muut tunneloidut yhteydet merkitään omina yhteyksinään vaikka ne käyttäisivätkin olemassa olevia fyysisiä linkkejä. (Hakala & Vainio 2005, 419.)

Julkiset palvelut, kuten web-, nimi- ja sähköpostipalvelimet, kuuluvat usein ydintasolle. Topologiassa niitä kannattaa käsitellä omana toimipaikkanaan, josta voidaan käyttää nimitystä demilitarisoitu alue. Näiden palveluiden tarkennus tehdään jakelutasolla. (Hakala & Vainio 2005, 419.)

Ydintason suunnittelussa päätetään käytettävistä julkisista IP-osoitteista sekä jaetaan toimipaikoille intranet-osoitesarjat. Samalla päätetään nimeämisjärjestelmästä, jossa määritellään perusperiaatteet laitenimien muodostamiseen sekä hakemistopalveluiden organisaatio ja organisaatioyksiköiden nimeämisestä. Nimijärjestelmän suunnitteluun

liittyy olennaisesti myös nimipalveluissa käytettävien vyöhykenimien suunnittelu sekä julkisten verkkonimien rekisteröinti. (Hakala & Vainio 2005, 419.)

Etuna näin suunnitellussa ydintasossa ei tarvitse ottaa kantaa aktiivilaitteisiin tai palvelimiin, vaan voidaan keskittyä kaapeleiden sekä muiden yhteyspalveluiden vertailuun ja kilpailutukseen. (Hakala & Vainio 2005, 419.)

3.2.2 Jakelutason suunnittelu

Jakelutason suunnittelussa jokaisesta toimipaikasta laaditaan oma looginen topologia. Siihen merkitään reitittimien tai reitittävien kytkinten erottamat lähiverkot ja niihin kuuluvat jakelutason palvelimet. Tyypillisesti tälle tasolle kuuluvat organisaation nimipalvelimet, hakemistopalvelimet, autentikointipalvelimet, toimipaikkakohtaiset tiedosto- ja sovelluspalvelimet sekä jakelutasoa suojaavat palomuurit. (Hakala & Vainio 2005, 419.)

Usein on myös järkevää sijoittaa toimipaikkakohtaiset etäkäyttöpalveluissa tarvittavat laitteet tälle tasolle. Julkisista palveluista, kuten www-, nimi-, ja sähköpostipalvelimista sekä niitä suojaavista palomuureista laaditaan oma looginen topologia. Tähän merkitään lähiverkot ja niitä yhdistävät kaapeloinnit sekä käytettävät protokollat. Mikäli jakelutasolla käytetään VPN-yhteyksiä tai VLAN-määrityksiä, nämä piirretään topologiaan omina loogisina yhteyksinä. (Hakala & Vainio 2005, 420.)

Kun toimipaikkakohtaiset loogiset topologiat on suunniteltu, suunnitelmaa tarkennetaan fyysisellä kaaviolla. Siinä suunnittelu viedään yksittäisten kaapeleiden ja aktiivilaitteiden porttien tasolle. Fyysisellä tasolla suunnitellaan käytettävien porttien nopeudet, käytettävät VLAN- ja VPN-määritykset sekä tarvittavat rinnakkais- ja varayhteydet. Laitteiden käyttämät nimet ja IP-osoitteet merkitään sekä loogiseen että fyysiseen kaavioon. Loogisiin topologioihin kannattaa merkitä myös verkkojen käyttämät IP-osoitealueet. (Hakala & Vainio 2005, 420.)

3.2.3 Liityntätason suunnittelu

Liityntätason suunnittelua tehdään yleensä fyysisten verkkokaavioiden tasolla. Verkkokaavioihin piirretään fyysinen kaapelointi jakamoineen, aktiivilaitteet sekä työasemat ja lähipalvelimet. Aktiivilaitteet ja jakamot kuvataan liitinten tasolla. Kapasiteetti vaatimukset merkitään porttikohtaisesti käytettävänä nopeutena. Looginen rakenne huomioidaan merkitsemällä VLAN-määritykset porttien läheisyyteen. VPN-yhteydet toteutetaan pääasiassa työasemiin asennettavien VPN-asiakasohjelmien avulla ja ne merkitään työasemien tietoihin. (Hakala & Vainio 2005, 420.)

Aktiivilaitteiden yhteydet jakelukerrokselle merkitään topologiaan. Suunnittelussa huomioidaan myös rinnakkais- ja varayhteydet merkitsemällä ne. Lähipalvelimet kuuluvat olennaisena osana liityntätason suunnitelmaan. Työasemien protokollia ei yleensä merkitä, koska niiden kirjaaminen topologioihin vaikeuttaisi luettavuutta. Suurissa organisaatioissa lähipalvelinten lisäksi liityntätasolle kuuluvat asetustenjakopalvelimet eli DHCP- ja BOOTP-palvelimet. (Hakala & Vainio 2005, 420–421.)

3.3 Verkon palvelut

Yksi suunnittelun kulmakivistä on verkossa tarjottavat palvelut. Tavoitteena on tarjota palvelut mahdollisimman pienellä aktiivilaitemäärällä. Käyttäjät tarvitsevat kuitenkin myös organisaation yhteisiä palveluja sekä muiden toimipaikkojen ja internetin tarjoamia palveluita. Niiden vaatimaan kaistanleveyteen ei aina riitä yleiskaapelointistandardin mukainen Ethernet-kaapelointi. Mikäli varayhteyksiä rakennetaan, vaatii sekin usein ylimääräisen kaapeliyhteyden. Se mitä palveluita verkossa tarvitaan tai tarjotaan määrittävät pitkälle aktiivilaitteiden ominaisuudet. (Hakala & Vainio 2005, 414.)

Myös palveluiden käyttämiseen tarvittavat protokollat vaikuttavat aktiivilaitteiden valintaan. Eikä unohtaa voi ylläpitoon tarvittavia palveluita, kuten nimipalvelut, asetustenjakelupalvelimet sekä autentikointipalvelut. (Hakala & Vainio 2005, 414.)

3.3.1 Laitteiston valitseminen

Aktiivilaitteiden suunnittelussa on otettava huomioon niiden tarjoamat protokolla tuet. Sopivia laitevaihtoehtoja haettaessa joudutaan selvittämään, vastaavatko niiden ominaisuudet tarvittuja. Niiden olisi hyvä vastata kysymyksiin:

- Tukevatko ne kuormituksen tasausta?
- Mitä suojausominaisuuksia niissä on?
- Onko niissä kaikki käytettävään protokollaan kuuluvat ominaisuudet?
- Mitä verkonhallintaprotokollia ne tukevat?
- Millä ohjelmistoilla niiden konfiguraatioita hallitaan?
- Tukevatko laitteet ulkoisia lokipalveluita?
- Miten ne voidaan suojata luvattomalta käytöltä?
- Mitä vikasieto-ominaisuuksia niissä on?

(Hakala & Vainio 2005, 414–415.)

Kuten aikaisemmin käsiteltiin, verkko koostuu pääsääntöisesti kytkimistä ja reitittimistä. Kytkinten ominaisuudet vaihtelevat aina hallitsemattomista plug-n-play-laitteista laajoilla hallintaominaisuuksilla varustettuihin reitittäviin kytkimiin. Vastaavasti yksinkertaisimmat reitittimet toimivat lähiverkon ja laajaverkon välisenä yhdyskäytävänä eivätkä sisällä erityisiä hallintaominaisuuksia. Tehokkaammat reitittimet on varustettu laajoilla hallintaominaisuuksilla ja ne mahdollistavat useiden eri protokollien käytön. (Hakala & Vainio 2005, 414–415.)

3.3.2 Kaapeloinnin valitseminen

Yleiskaapelointi on nimensä mukaisesti suunniteltu tukemaan erilaisia sovelluksia, kuten äänensiirtoa, datansiirtoa ja kuvansiirtoa. Lähtökohtana on kiinteä kaapelointi, joka tukee kaikkia näitä sovelluksia. Yleiskaapeloinnissa käytetään joko valokaapeleita tai kierrettyjä parikaapeleita. Järjestelmässä suositellaan käytettäväksi monimuotokuituja valokaapeleissa, mutta ominaisuuksiltaan parempi yksimuotokuitu on pitkälti syrjäyttänyt monimuotokuidut asennuksissa. (Hakala & Vainio 2005, 116–117.)

Parikaapelit on jaettu puolestaan kategorioihin 5–7, jotka ovat yleisesti käytössä nykyisin. Lähes kaikki kerroskaapeloinnit tehdään nykyään kategorian 6 kaapeleilla, joilla

saavutetaan gigabitin siirtonopeus sekunnissa. Tällä kategorialla on myös valmius kymmenen gigabitin siirtonopeuteen sekunnissa. Valokaapelia käytetään kerrosten välissä sekä palvelinten ja aktiivilaitteiden välisissä yhteyksissä. Liityntätasolla aktiivilaitteiden ja työasemien välille asennetaan Cat 7 -kaapelit, joiden standardoitu nopeus on 10 gigabittiä sekunnissa. Tämä takaa tulevaisuudessa nopeuden kasvattamisen, kunhan työasemat tukevat sitä. Tasojen väliset yhteydet aktiivilaitteissa hoidetaan valokaapelointia käyttäen. (Hakala & Vainio 2005, 117–118, 129.)

3.4 Tietoturva

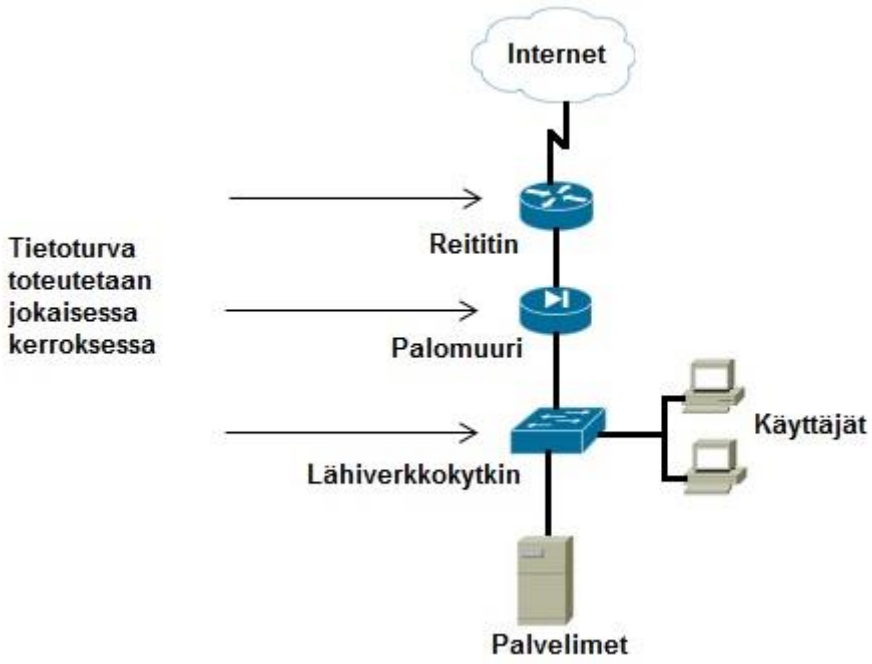
Tieto on yrityksen keskeinen voimavara ja avain menestykseen. Siksi sitä on suojattava samalla tavalla kuin yrityksen fyysistä omaisuutta, työntekijöitä tai brändiä. Nykyisin yritykset ovat lähes poikkeuksetta verkossa ja edellytys selviytymiselle tässä verkostoituneessa maailmassa on tietoturva. (Järvinen 2002, 111.)

Yrityksen tietoturvalta edellytetään sisältö- ja laatuvaatimuksia, jotta yritys pääsisi mukaan yhteistyö- ja alihankintasopimuksiin. Elleivät asiat ole kunnossa, sopimuksia ei synny. Toisaalta retuperälle jätetty tietoturva voi kostautua vahingonkorvauksina tai sopimussakkoina, joista kumpikaan ei paranna yrityksen liiketulosta eikä imagoa. (Järvinen 2002, 111.)

Tietoturva mielletään helposti vain tietokoneisiin ja tekniikkaan liittyväksi käsitteeksi, jossa tavoitteena on torjua hakkerit ja virukset sekä taata säännöllinen varmuuskopiointi. Tietoturvakäsitteen laajempi merkitys paljastuu vasta tarkastelemalla kaikkia siihen liittyviä osa-alueita. (Järvinen 2002, 112.)

3.4.1 Tietoturvakäsitteen osa-alueet

Kerrosteinen tietoturva – Verkossa, jossa tietoturva on toteutettu kerrosrakenteen mukaisesti, on huomioitu, että yksittäinen puolustuksen kohta vikaantuu ennemmin tai myöhemmin. Kuviossa 3 on hyvin suunniteltu ratkaisu, jossa tietoturva on toteutettu johdonmukaisesti mahdollisimman monessa verkon eri pisteessä. Verkon kerrosteinen tietoturva on keskeinen osa yrityksen verkkoa. (Thomas 2005, 86.)



KUVIO 3. Kerrosteisen tietoturvan pisteet (Thomas 2005, 86.)

Pääsynvalvonta – Verkko on viime kädessä verkonhaltijan vastuulla ja siksi hän päättää verkkoon pääsystä. Eräs suositeltava käytäntö pääsynvalvonnassa on lähteä siitä ajatuksesta, että kaikki muu paitsi yrityksen toiminnan kannalta oleellinen liikenne estetään. Tästä käytetään myös nimitystä ”Policy of Least Privilege” eli pienimpien mahdollisten oikeuksien käytäntö. Tämä asetus on oletuksena Ciscon palomuureissa. (Thomas 2005, 86.)

Rooleihin perustuva tietoturva – Päätettäessä pääsystä ja oikeuksista eli luotettavuudesta eräs käyttökelpoisimmista malleista perustuu käyttäjän rooliin organisaatiossa. Esimerkiksi web-sivujen kehittäjälle on ilmeisen oleellista päästä organisaation websivustoon, hallinnon assistentille sen sijaan ei. (Thomas 2005, 87.)

Käyttäjien tietoisuus – Kerrotaan paljon tarinoita käyttäjistä, jotka kirjoittavat muistiin salasanansa, muuttavat niitä viisi kertaa peräkkäin ja käyttävät sitten alkuperäistä salasanaansa uudelleen. Kyse ei ole siitä, että käyttäjät tarkoituksella pyrkisivät kiertämään tietoturvaa. He vain eivät ymmärrä sen tarkoitusta ja osasta se voi tuntua it-osaston kiusanteolta. On tärkeää, että käyttäjät saadaan koulutuksen kautta tietoisiksi tietoturvan merkityksestä. Eräs hyvä keino saada käyttäjät mukaan koulutustilaisuuksiin kuulemaan tietoturvan tärkeydestä on tarjota kahvia ja pullaa. Tämä menetelmä vetoaa perustarpeisiin, mutta on myös tehokas ja hauska sekä tekee koulutuksen järjestäjästä

hyvin suositun henkilön. On erittäin tärkeää, että käyttäjät todella ovat tietoisia turvallisuudesta ja tukevat tietoturvakäytäntöjä. (Thomas 2005, 87.)

Tarkkailu – Yleensä tämä jää vähimmälle huomiolle tietoturvan osa-alueista. Monet organisaatiot uskovat, että riittää, kun tietoturva on järjestetty kerran kuntoon. Monesti unohtuu, että järjestelmien tarkkailu on tärkeää myös. Vain järjestelmän tarkkailulla voidaan varmistaa, että turvallisuus säilyy ja että ne eivät ole hyökkäyksen kohteena. On erittäin suositeltavaa ottaa verkon tietoturvaratkaisu suunnitteluun mukaan hyökkäyksien tarkkailu menetelmiä, kuten tunkeutumisen havaitsemisjärjestelmät IDS. (Thomas 2005, 87.)

Tunkeutumisen havaitsemisjärjestelmät ovat ikään kuin verkon hälytysjärjestelmiä. Verkko on suojattu, mutta ilman IDS:n kaltaista hälytysjärjestelmää ei voida koskaan tietää, yrittikö hyökkääjä päästä verkkoon. Tunkeutumisen havaitsemisen tavoitteena on tarkkailla verkon resursseja ja pyrkiä havaitsemaan poikkeuksellinen käyttäytyminen, sopimaton toiminta ja hyökkäykset tai pysäyttää tunkeutuminen. IDS voidaan sijoittaa verkossa useaan eri paikkaan turvallisuuden ja suojauksen parantamiseksi. Nykyisin IDS:n päätyypit ovat verkko- ja isäntäpohjainen. Ne poikkeavat toisistaan tekniikaltaan, jolla ne havaitsevat ja viivästyttävät vihamielistä toimintaa. Verkossa tulisi käyttää molempia, jotta kerrosteisessa puolustusmallissa saavutettaisiin paras mahdollinen tehokkuus. (Thomas 2005, 326–327.)

Verkkopohjainen tunkeutumisen havaitsemisjärjestelmä NIDS sijaitsee suoraan verkossa ja vahtii kaikkea verkossa kulkevaa liikennettä. NIDS on tehokas sekä saapuvan ja lähtevän liikennevuon että samassa tai eri verkkosegmenteissä olevien isäntien välisen liikenteen valvonnassa. NIDS sijoitetaan yleensä palomuurien ja VPN-yhdyskäytävien molemmille puolille, jolloin sen on mahdollista mitata kyseisten turvalaitteiden tehokkuutta ja toimia yhdessä niiden kanssa. (Thomas 2005, 327.)

Isäntäpohjainen tunkeutumisen havaitsemisjärjestelmä HIDS on erikoissovellus, joka asennetaan tietokoneeseen, yleensä palvelimeen, ja se vahtii kaikkea kyseisen palvelimen saapuvaa ja lähtevää liikennettä sekä tarkkailee tiedostojärjestelmän muutoksia. HIDS on erittäin tehokas ratkaisu kriittisiin, internetiin yhteydessä oleviin sovelluspalvelimiin, kuten web- tai sähköpostipalvelimet, koska se pystyy valvomaan sovelluksia niiden lähteessä ja suojelemaan niitä. (Thomas 2005, 327.)

Todella tehokas kerrosteinen puolustus sisältää sekä NIDS- että HIDS-järjestelmän, jolloin saavutetaan organisaation tietoliikenteen hyvä näkyvyys ja hallinta. IDS-järjestelmät tarjoavat organisaatiolle myös hyvät tiedot niiden turvallisuusjärjestelmien ja tietoturvaan tehtyjen investointien tehokkuudesta. Markkinoilla on nykyisin tarjolla IDS-järjestelmiä, joissa on valtava määrä ominaisuuksia. Organisaation tulisi huolellisesti arvioida mitä ominaisuuksia tarvitsee perinteisen tapahtumalokituksen lisäksi. (Thomas 2005, 327.)

Järjestelmäpäivitykset – Järjestelmien päivittäminen on perustehtävä, jonka järjestelmänhaltijat usein aikataulukiireissään unohtavat. Onneksi käyttöjärjestelmät nykyisin osaavat muistuttaa saatavissa olevista päivityksistä. (Thomas 2005, 87.)

3.4.2 Tietoturvapolitiikka

Tietoturvapolitiikka on yrityksen tietoturvan kulmakivi. Politiikka on yrityksen johdon hyväksymä näkemys tietoturvan päämääristä, periaatteista ja toteuttamisesta. Sitä kautta johto linjaa sen, miten tietoturva-asioita tullaan kehittämään. Kun johto sitoutuu politiikkaan, se velvoittaa myös kaikkia työntekijöitä. (Järvinen 2002, 113.)

Tietoturvapolitiikalle ei ole mitään yksikäsitteistä määrittelyä. Se voi olla muutaman sivun tiivistetty kuvaus tietoturvaan liittyvistä asioista, joka voidaan laittaa vaikka yrityksen nettisivulle. Tällöin se rinnastetaan ympäristö-, henkilöstö- ym. politiikkaan. Joissakin yrityksissä tietoturvapolitiikka on luokiteltu salaiseksi, koska se sisältää yksityiskohtaisia toimintaohjeita ja menettelytapoja siitä, miten tavoitteisiin pyritään. Yleensä on kuitenkin parempi erotella käytännön ohjeet omiksi dokumenteiksi, jotka jaellaan vain tietoa tarvitseville. (Järvinen 2002, 113.)

Organisaatio joutuu ennemmin tai myöhemmin kohtaamaan tietoturvaan liittyviä huolenaiheita. Ehkä järjestelmät ovat joutuneet hyökkäyksen kohteiksi tai on voitu havaita, että murtautuminen on ja vahinko ovat jo tapahtuneet. On parempi muodostaa toimenpideryhmä ja harjoitella sen toimintaa etukäteen kuin vasta silloin, kun tilanne on jo päällä ja kärjistynyt. Suunnittelutyö tulee siis tehdä nyt, hyödyt kyllä seuraavat perässä. Harjoitus tekee mestarin ja kuivaharjoittelu voi auttaa havaitsemaan tietoturvasuunni-

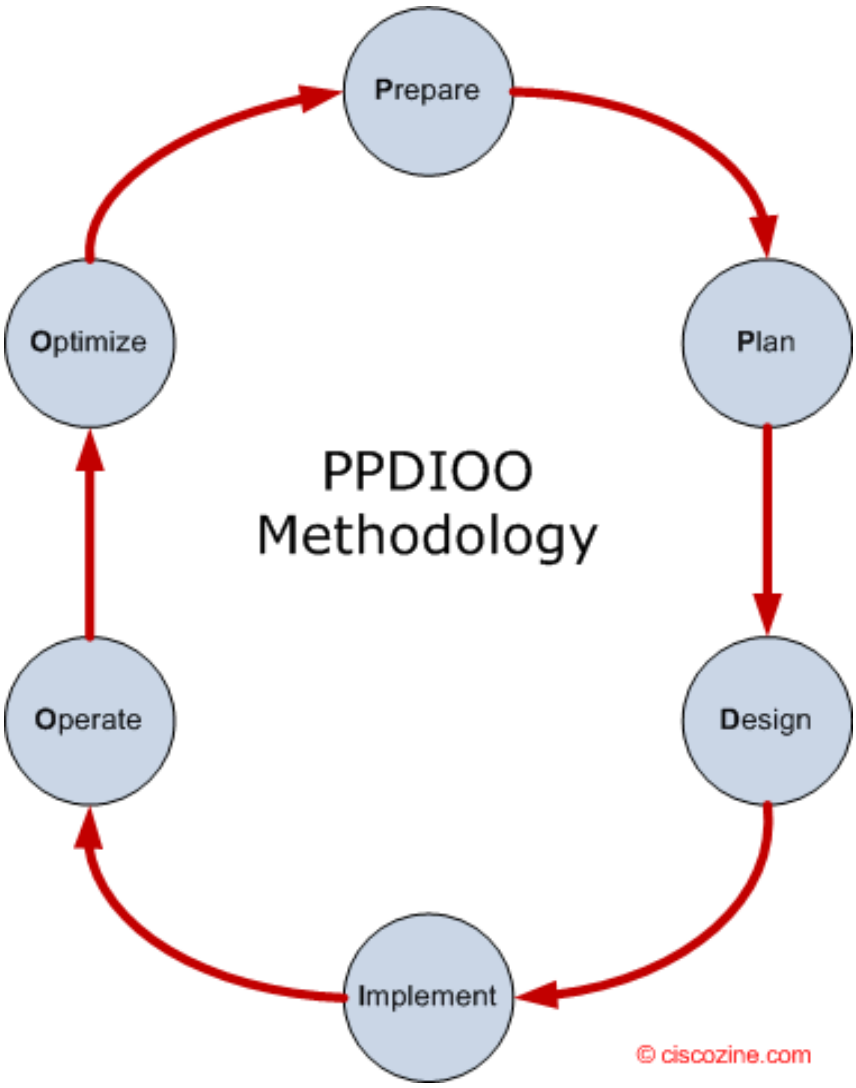
telman heikot kohdat, jotka eivät suunnitelmaa kirjottaessa ole tulleet esille. (Thomas 2005, 88.)

4 VERKON YLLÄPITO JA KEHITTÄMINEN

Kun tietojärjestelmäprojektit ovat päässeet käyttöönottovaiheeseen, niin alkaa järjestelmien ja siihen kuuluvien verkkojen rutiininomainen ylläpito. Sen aikana laaditaan dokumentit järjestelmään tehdyistä muutoksista ja laajennuksista. Dokumentointiin kuuluvat mm. käyttäjä- ja käyttöoikeusasetukset, aktiivilaitteiden konfiguraatiomuutokset sekä ristiinkytkentätaulukot ja verkon yhteyskaaviot. Ylläpitovaiheessa suoritetaan myös liikenne- ja kuormitusanalyysejä sekä kerätään lokitiedostoja. Ennen tätä vaihetta tarvitsee useita muita vaiheita suorittaa, oli kyseessä täysin uusi verkko tai vanhan verkon päivittäminen. (Hakala & Vainio 2005, 411.)

4.1 Ciscon elinkaariajattelumalli

Ciscon verkon elinkaariajattelumalli auttaa ymmärtämään mitä verkossa pitäisi tapahtua kussakin vaiheessa. Tämä on tärkeää, jotta yritys tai konsultti käyttää oikein elinkaariajattelua ja saa parhaimman hyödyn. Seuraavaksi käydään läpi vaihe vaiheelta, mitä jokaisessa vaiheessa tapahtuu sekä mitä yleensä niissä tuotetaan tai suoritetaan. Nämä vaiheet ovat esitetty kuviossa 4 sekä ajattelumallin kiertokulku. Vaiheet ovat suomennettuna ylhäältä aloittaen esitutkimus, määrittely, suunnittelu, toteutus, käyttöönotto ja optimoi. (Wilkins, 2011; Sivasubramanian, Frahim, & Froom, 2010.)



KUVIO 4. Ciscon verkon elinkaarimalli (http://www.ciscozine.com/2009/01/29/the-ppdioo-network-lifecycle)

Esitutkimusvaiheen käyttö riippuu yrityksen nykytilasta. Ensimmäinen tapa edellyttää, että yhtiö on tehnyt vähän tai ei ollenkaan tutkimusta liiketoiminnan perustamisen vaatimuksiin, mm. teknologia visio ja teknologian strategia. Toinen tapa olettaa, että yritys on jo perustettu, ja tämä on kertaus esitutkimusvaiheen läpi sekä nykyisiin suunnitelmiin voidaan tehdä päivityksiä. (Wilkins, 2011.)

Yleisesti ottaen esitutkimusvaiheessa yritys kehittää liiketoiminnan vaatimuksia, teknologia visiota ja teknologia strategiaa. On erittäin tärkeää, että nämä vahvistetaan ennen kuin edetään, jotta voidaan varmistua, että verkko on kehitetty niin lähelle liiketoiminnan vaatimuksia kuin mahdollista. (Wilkins, 2011.)

Jos tämä ei ole ensimmäinen iterointi esitutkimusvaiheessa, sitten tarvitsee tarkistaa nykyisen liiketoiminnan edellytykset aiemmin kehitettyyn. Jos muutoksia havaitaan, teknologia visioissa tai strategiassa, pitäisi muutokset vastata näihin uusiin olosuhteisiin. Tämän analyysin lopputulosta käytetään kehittämään erittäin korkean tason käsitteellinen arkkitehtuuri ehdotetusta verkosta. Suositellut ominaisuudet ja toiminnot, jotka on ehdotettu, tulisi validoida ennen käyttöönottoa. Tyypilliset suoritteet tästä vaiheesta ovat korkeatasoinen suunnitelma, asiakkaiden vaatimus dokumentit ja nykytila arviointi. (Wilkins, 2011.)

Määrittelyvaiheessa, kuten esitutkimusvaiheessakin, sen käyttö riippuu organisaation verkon tilasta. Seuraava askel on hankesuunnitelman laatiminen. Mikäli verkkoa ei ole olemassa, tämän määrittelyvaiheen aikana laaditaan verkon vaatimukset, jotka kirjataan hankesuunnitelmaan. Siitä pitää ilmetä ennen seuraavia vaiheita, resurssien käyttö niin kustannus kuin laitteet, verkon turvallisuussuunnitelma ja aikataulutus, joiden tarvitsee vastata esitutkimusvaiheen liiketoiminnan vaatimuksia. (Wilkins, 2011.)

Mikäli verkko on olemassa, niin hankesuunnitelman tarkoitus on kehittää tai päivittää, mutta vasta sitten, kun tarkastus verkosta, sivustojen ja operatiivisesta toimivuudesta on suoritettu. On tärkeää, että perusteellinen tarkastus on suoritettu, jotta voidaan varmistua, että muutokset eivät vaikuta verkon käytettävyyteen tai alenna verkon kapasiteettia, näin verkon päivitys onnistuu ilman suurempia ongelmia. Tyypillisiä dokumentteja määrittelyvaiheesta ovat sivustojen vaatimuskuvaukset, hankesuunnitelma, palautelomake ja asiakkaiden vaatimuskuvaukset sekä palautteet. (Wilkins, 2011.)

Suunnitteluvaiheen aikana organisaatio kehittää tai päivittää kattavasti verkkosuunnitelmaa. On tärkeää, että aikaisemmissa vaiheissa kerätty informaatio ja suunnitelma vastaavat toisiaan sekä liiketoiminnan ja teknisiin vaatimuksiin. Mikäli kaikki on suoritettu oikein, suunnitelma tarjoaa verkon, joka vastaa yrityksen tarpeisiin ja täyttää tai ylittää odotukset saatavuudesta, luotettavuudesta, turvallisuudesta, skaalautuvuudesta ja suorituskyvystä. (Wilkins, 2011.)

Tässä vaiheessa on myös erilaisia asiakirjoja, joita kehitetään prosessin ajan. Ne ohjaavat sijoittelussa, konfiguroinnissa sekä laitteiden ja palveluiden toteuttamisessa. Tyypillinen dokumentti on niin sanottu matalan tason suunnitelma. Tämä suunnitelma sisältää

tiedot verkon laitteista, protokollista ja palveluista yksityiskohtaisesti. Ciscon sivuilta saa ladattua valmiin pohjan osoitteesta http://www.cisco.com/global/EMEA/IPNGN/docs/templates/LLD_Template_7April05.doc. (Wilkins, 2011.)

Toteusvaiheessa on olemassa useita eri menetelmiä, joita käytetään. Yleensä on hyvä asentaa ja konfiguroida testiympäristö, jota käytetään simuloimaan eri osat tai lisäykset verkon suunnittelussa. Tällä menetelmällä järjestelmänvalvojat pystyvät löytämään mahdolliset ongelmat. Jos niitä löytyy, nämä ongelmat voidaan ratkaista testiympäristössä ennen kuin täytäntöön pano jatkuu. Kun kaikki asiat ovat työstetty testiympäristössä, täysimittainen täytäntöönpano voi alkaa, tietenkin riippuen täytäntöönpanon koosta. Matkalla voi ilmetä useita logistisia kysymyksiä, jotka tarvitsee selvittää tänä aikana. Esimerkiksi se on määritettävä kuka on vastuussa käyttöönotosta, konfiguraatiosta, testauksesta, ja verkon toiminnasta näissä eri vaiheissa. Yhtiön on myös varmistettava, että kaikki yhdentämistehtävät nykyisen verkon kanssa hoidetaan huolellisesti, jotta käynnissä oleva toiminta häiriintyy mahdollisimman vähän. (Wilkins, 2011.)

Kun verkko on toteutettu, sarja testejä pitäisi suorittaa, jotta varmistutaan uuden verkon toimivuudesta odotetulla ja suunnitellulla tavalla. Jos jotain ongelmia löytyy, se on parasta, että ne käsitellään mahdollisimman varhaisessa täytäntöönpanon vaiheessa, mahdollisimman tarkasti, jotta vaikutus jäisi niin vähään osaan verkkoa kuin mahdollista. Tyypilliset suoritteet tästä vaiheesta ovat verkkovalmis käyttöön testi ja raportti sekä toteutusloki. (Wilkins, 2011.)

Käyttöönottovaihe on ylivoimaisesti pisin PPDIOO:n vaiheista. Tämä johtuu siitä, että tähän vaiheeseen mennessä yritys on toiminut ilman merkittäviä muutokset verkkoon. Tämän vaiheen aikana, yritys käyttää suurimman osan varoista verkon hallinnoinnista, joka sisältää proaktiivista ja reaktiivista seurantaa, suorituskyvyn hallintaa, ongelmien hallintaa, turvallisuuden hallintaa ja kapasiteetin suunnittelua ja seurantaa monien muiden lisäksi. Kaikki pienet lisäykset tai muutokset esiintyvät myös tässä vaiheessa. Tyypillisiä asiakirjoja tästä vaiheesta ovat perussyyanalyysimenetelmä raportit, MAC-raportit ja tukisopimukset. (Wilkins, 2011.)

Optimointivaihe voi tapahtua milloin tahansa, kun verkko on toiminnassa. Yleensä se tapahtuu joko, kun on ollut vähäisiä tai suuria muutoksia liike- tai teknisissä vaatimuksissa tai aikataulussa. Tämän vaiheen aikana, nykyisen liiketoiminnan ja teknisiä vaati-

muksia verrataan käytettävään verkkoon, joka alun perin suunniteltiin. Jos muutoksia suositellaan, vaiheet aloitetaan uudelleen alusta johdonmukaisuuden ja jatkuvan hyvän suunnitelman varmistamiseksi. (Wilkins, 2011.)

4.2 Päivittäminen

Ylläpitovaiheen yksi tärkeimmistä tehtävistä on järjestelmien päivittäminen. Kaikkien käyttöjärjestelmien turvallisuus perustuu nykyisin päivityksiin. Oli kyseessä sitten aktiivilaitteiden Cisco IOS tai työasemien Windows -käyttöjärjestelmä. Säännöllisyys on tietoturvan ensimmäinen edellytys. (Järvinen 2006, 15.)

Päivittämisestä on tullut yhtä arkista rutiinia kuin siivouksesta. Vähintään kerran viikossa jokin ohjelma tai laite ilmoittaa, että päivitys saatavissa. Päivittäminen on tarpeellista, koska laitteet ja ohjelmistot tuodaan myyntiin keskeneräisinä.. Kiireen vuoksi niihin jää virheitä, joita joudutaan sitten paikkailemaan näillä päivityksillä. Joskus päivittäminen voi tuoda uusia ominaisuuksia, esimerkiksi tuen jollekin uudelle protokollalle tai tekniikalle, jota ei vielä tuotteen valmistuessa ollut olemassa. (Järvinen 2006, 15.)

Tällainen päivittäminen pidentää tuotteen käyttöikää ja on siksi niin sanotusti huonoa bisnestä. Valmistajan kannalta parempi ratkaisu olisi saada asiakas ostamaan kokonaan uusi laite päivittämisen sijaan. Tästä syystä jokaisella laitteella on elinikä eli aika, jonka aikana valmistaja julkaisee päivityksiä. Päivityksen loppuvat, kun tuote tulee elinikänsä päähän. Tällä viestitään asiakkaalle, että olisi aika ostaa uusi tuote. Yleisimmin käytetyt Microsoftin Windows- ja palvelinkäyttöjärjestelmät käyttävät automaattista päivitystä, joka voidaan järjestelmänvalvojan toimesta asettaa myös keskitetysti. (Järvinen 2006, 15, 31–32.)

4.3 Elinkaariajattelun hyödyt

Verkon elinkaariajattelumalli tarjoaa useita keskeisiä etuja pitää suunnitteluprosessia systemaattisena. Tärkeimmät syyt elinkaariajattelun käyttöönottamiseen suunnittelussa ovat kokonaiskustannuksien väheneminen verkon hallinnoinnissa, lisääntyvä verkon

käytettävyys, parantaa liiketoiminnan ketteryyttä ja nopeat yhteydet sovelluksiin ja palveluihin. (Sivasubramanian ym., 2010.)

Kokonaiskustannukset verkon hallinnassa ovat erityisen tärkeitä nykypäivän liiketoimintaympäristössä. Kustannustehokkuus IT-kuluissa on jatkuvasti yrityksen avainhenkilöiden suurennuslasin alla. Kuitenkin oikea verkon elinkaariajattelu auttaa alentamaan kustannuksia toimilla, jotka ovat verkon yksilöinti ja validointi teknologian vaatimuksiin, suunnittelu infrastruktuurin muutokset ja resurssitarpeet, onnistunut toteuttaminen, verkon tehostaminen ja sitä tukeva henkilöstö sekä kulujen vähentyminen tehostamalla toiminnallisia prosesseja ja työkaluja. (Sivasubramanian ym., 2010.)

Verkon toimivuus on aina ollut etusijalla yrityksissä. Kuitenkin verkon käyttökatkot voi johtaa tulojen menetykseen. Esimerkkejä verkon seisokeista, joista saattaa aiheutua tulojen menetystä ovat verkon vikaantuminen tai suuri käyttäjämäärä samanaikaisesti, jotka estävät kaupankäynnin tai kyvyttömyyden käsitellä luottokorttien transaktioita. Verkon elinkaariajattelu parantaa korkean käytettävyyden verkkoja. (Sivasubramanian ym., 2010.)

Tärkein hyöty kaikista on dokumentoiminen. Jokaisessa vaiheessa oikein laaditut asiakirjat edes auttavat verkon ylläpitämistä sekä kehittämistä. Ilman dokumentointia olisi erittäin vaikeaa todentaa verkon toiminnallisuutta oikein, koska ei ole olemassa referenssejä miten sen pitäisi toimia. Tämän ajattelumallin avulla jokainen verkon ylläpitäjä pystyy kehittämään verkkoa entistä luotettavammaksi ja tehokkaammaksi eri tilanteissa.

5 POHDINTA

Työ oli yllättävän laaja-alainen ja rajausta jouduttiin käyttämään rankalla kädellä. Osan haasteista toi yrityksen puute. Kuvitteelliselle yritykselle ei ole helppo suunnitella uutta verkkoa, koska ei ole vanhaakaan olemassa mille tehdä työssä kuvatut analyysit, joiden pohjalta voitaisiin kehittää uuden verkon ominaisuudet vaaditulle tasolle. Lähtökohdat työlle eivät olleet kovin loistavat yrityksen kuvitteellisuudesta johtuen. Tämä johti siihen, että työssä keskityttiin lähinnä suunnittelun eri vaiheisiin. Näistä osa-alueista jouduttiin jättämään kuvitteellisuuden vuoksi pois. Silti työssä onnistuttiin keräämään tarvittavat tiedot verkon suunnittelusta ja miten siihen kannattaa valmistautua.

Liitteessä 1 oleva topologia kuvaa verkon toimintoja hyvin, vaikka siinä ei ole kaikkia yksityiskohtia mitä tässä työssä käsiteltiin. Topologiasta pystytään erottamaan eri tasot verkossa niin osastokohtaisesti kuin koko verkon osalta. Siitä ilmenevät osastot, reititysprotokollat, virtuaaliset lähiverkot sekä osoiteavaruudet. Näillä tiedoilla pystytään luomaan toimiva verkko. Kehittämistä löytyy tietoturvasta, joka puuttuu kaaviosta, simulointi ohjelman rajallisuuden takia.

Liitteessä 2 on kustannusarvio, joka todella on vain arvio. Luonnollisesti kuvitteellisella yrityksellä ei ole toimitiloja, jolloin voisi laskea tarkasti tarvittavan kaapeli määrän. Kustannusarvion tarkoitus on lähinnä toimia raamina budjettilaskuille, josta jatkossa pystytään kehittämään toimiva laskuri samassa tilanteessa oleville yrityksille.

Haastavinta työssä oli löytää tuoretta lähdemateriaalia, kun tekniikat kehittyvät niin valtavalla nopeudella eteenpäin. Muutama artikkeli, jotka ovat melko tuoreita, onnistuttiin kaivamaan internetin syövereistä. Ne ovat luotettavista ja alalle vakiintuneista uutispalveluista. Vaikka kirjallisuuden lähteet ovat jo iäkkäitä, perusideat näissä ovat paikkansa pitäviä.

Toivottavasti tämä työ tarjoaa niin asiasta tietämättömälle kuin asiaan perehtyneelle uusia näkökulmia tietoverkon suunnitteluun ja sen vaatimuksiin. Nykyisin ei voi riittävästi korostaa tietoturvan tärkeyttä suunnittelussa. Omana huomiona voisin vielä todeta aikataulutuksen. Määrittely- ja suunnitteluvaiheeseen kannattaa varata reilusti aikaa, sillä onhan hyvin suunniteltu jo puoliksi tehty.

LÄHTEET

Briscoe, N. 2000. Understanding The OSI 7-Layer Model. ITP 7/2000, 13-14 http://memberfiles.freewebs.com/61/55/58745561/documents/OSI.pdf

Digitoday. 2013. Pure pölyä valokuitu: tieto kiitää melkein valon nopeudella ilma-kuidussa. Julkaistu 27.3.2013. Luettu 19.4.2013. http://www.digitoday.fi/tiede-ja-teknologia/2013/03/27/pure-polya-valokuitu-tieto-kiitaa-melkein-valon-nopeudella-ilmakuidussa/20134566/66

Hakala, M. & Vainio, M. 2005. Tietoverkon rakentaminen. Jyväskylä: Docendo Finland Oy

Järvinen, P. 2006. Paranna tietoturvaasi. Jyväskylä: Docendo Finland Oy

Järvinen, P. 2002. Tietoturva & yksityisyys. Jyväskylä: Docendo Finland Oy

Lammle, T. 2011. CCNA: Cisco Certified Network Associate Review Guide (640-802). Hoboken NJ, USA: Sybex.

Sivasubramanian, B., Frahim, E. & Froom, R. 2010. Analyzing the Cisco Enterprise Campus Architecture. Cisco Press. Luettu 1.5.2013 http://www.ciscopress.com/articles/article.asp?p=1608131&seqNum=3

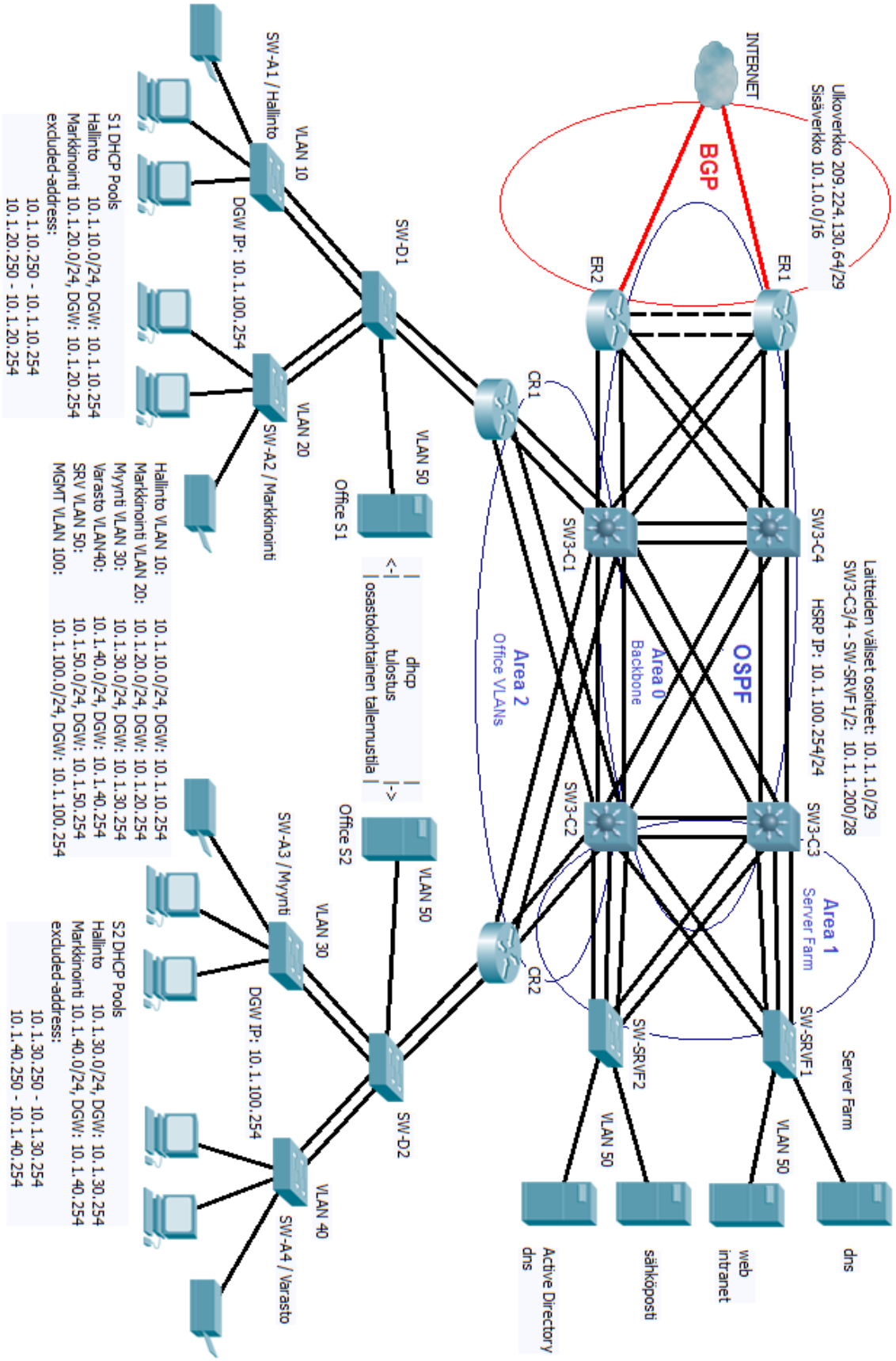
Thomas, T. 2005. Verkkojen tietoturva. Suom. Holttinen, J. Helsinki: IT Press. Alkuperäinen teos Network Security first-step. 2004.

Pitkänen, J. 2010. Sadan gigabitin ethernet-standardi valmistui. Tietokone. Julkaistu 23.6.2010. Luettu 4.5.2013. http://www.tietokone.fi/uutiset/sadan_gigabitin_ethernet_standardi_valmistui

Wilkins, S. 2011. Cisco's PPDIOO Network Cycle. Cisco Press. Luettu 1.5.2013. http://www.ciscopress.com/articles/article.asp?p=1697888&seqNum=2

LIITTEET

Liite 1. Verkon loogisen topologian perusmalli



Liite 2. Kustannusarvio

Taso	Laite	Tuote	Määrä	á-hinta	Yhteensä	Lisätietoja
Access / liityntä	Kytkin	WS-C3750X-24P-L	6	1 700,00 €	10 200,00 €	http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps6406/data_sheet_c78-584733_ps10744_Products_Data_Sheet.html
Distribution / jakelu	Kytkin	WS-C3750G-24TS-E1U	2	3 500,00 €	7 000,00 €	
Core / ydin	Kytkin	WS-C4948-10GE	4	4 500,00 €	18 000,00 €	http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps6021/ps6230/prod_bulletin0900aecd80246560.html
Distribution / jakelu	Reititin	CISCO2911/K9	2	950,00 €	1 900,00 €	http://www.cisco.com/en/US/products/ps10540/index.html
Core / ydin	Reititin	CISCO3925/K9	2	3 100,00 €	6 200,00 €	http://www.cisco.com/en/US/products/ps10542/index.html
Access / liityntä	Parikaapeli	Cat 7 S/FTP kela (100m)	10	125,00 €	1 250,00 €	http://www.verkkokauppa.com/fi/product/6081/dfkbf/Fuj-tech-Cat7-S-FTP-kaapelikela-100-m-oranssi
Distribution / jakelu	Parikaapeli	Cat 7 S/FTP kela (100m)	10	125,00 €	1 250,00 €	http://www.verkkokauppa.com/fi/product/6081/dfkbf/Fuj-tech-Cat7-S-FTP-kaapelikela-100-m-oranssi
Core / ydin	Valokuitu	Monimuoto LC/LC (50m)	10	250,00 €	2 500,00 €	
Kaikki	Kaikki	Asennuspalvelu e/h	24	60,00 €	1 440,00 €	
			70		**49 740,00 €**	